METHODS AND APPARATUS FOR SELECTIVE ENCRYPTION AND DECRYPTION OF POINT TO MULTI-POINT MESSAGES

ABSTRACT OF THE DISCLOSURE

Methods and systems for selectively encrypting and decrypting messages transmitted on a channel of a communication network, such as a broadcast channel, are provided. Group encryption keys are provided for one or more services utilizing the broadcast channel to communicate messages. A message associated with a particular service first receives an error check value, such as a cyclical redundancy check (CRC) value generated from the unencrypted message. The message is then encrypted using the group encryption key for the service and the CRC is added to the encrypted message and transmitted with a broadcast address of the communication network. A receiver then receives the message and determines that the CRC indicates an error (as it is generated from the encrypted message rather than the unencrypted message). The receiver then decrypts the message using the group encryption key for the service (assuming the receiver is authorized to receive the service, i.e., has access to the group encryption key) and generates a CRC from the decrypted message. If this CRC matches the CRC received with the message, the receiver recognizes the message as being associated with the corresponding service and processes the message accordingly. Where multiple services are supported and the receiver has a corresponding plurality of group encryption keys, each encryption key can be tested until a CRC without error is provided thereby indicating the service with which the message is associated.